UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

* * *

UNITED STATES OF AMERICA, Plaintiff, v. WEI SENG PHUA, et al., Defendants.	Case No. 2:14-cr-00249-APG-PAL
IN RE APPLICATION FOR SEARCH WARRANT FOR DEVICE 1 KNOWN AS AN APPLE IPAD MODEL A1455, SERIAL NUMBER DLXJRF5DF19M	Case No. 2:15-mj-0262-PAL Case No. 2:14-mj-0611-PAL
IN RE APPLICATION FOR SEARCH WARRANT FOR DEVICE 2 KNOWN AS AN APPLE IPHONE MODEL A1530, IMEI NUMBER 358030059205968	Case No. 2:15-mj-0263-PAL Case No. 2:14-mj-0612-PAL
IN RE APPLICATION FOR SEARCH WARRANT FOR DEVICE 3 KNOWN AS AN APPLE IPHONE MODEL A1530, IMEI 358030054212647	Case No. 2:15-mj-0264-PAL Case No. 2:14-mj-0613-PAL
IN RE APPLICATION FOR SEARCH WARRANT FOR DEVICE 4 KNOWN AS AN APPLE IPAD MODEL A1432, SERIAL NUMBER F87L6RPKF196	Case No. 2:15-mj-0265-PAL Case No. 2:14-mj-0614-PAL
IN RE APPLICATION FOR SEARCH WARRANT FOR DEVICE 5 KNOWN AS AN APPLE IPAD MODEL A1474, SERIAL NUMBER DLXLL11JFK17	Case No. 2:15-mj-0266-PAL Case No. 2:14-mj-0618-PAL
IN RE APPLICATION FOR SEARCH WARRANT FOR DEVICE 6 KNOWN AS	Case No. 2:15-mj-0267-PAL Case No. 2:14-mj-0619-PAL

AN APPLE IPAD MODEL A1454, SERIAL NUMBER F4KK8049F196

The government submitted six ex parte search warrant applications to me on February 19, 2015. The applications seek search warrants directing Apple to assist the Federal Bureau of Investigation in their search of four iPads and two iPhones seized in a search conducted on July 9, 2014, pursuant to a search warrant issued by the Honorable Nancy J. Koppe. Judge Koppe issued a warrant authorizing the search of Villas 8881, 8882 and 8888 at Caesars Palace under Case No. 2:14-mj-0458-NJK. The warrant authorized the search and seizure of evidence including all cell phones, Blackberries, iPhones, iPads and other electronic devices, laptop and desktop computers and other specified computer equipment and peripheral devices.

I reviewed these six search warrant applications, decided not to issue them, and had staff notify the government counsel of my decision. Government counsel requested a meeting to explain the government's position that these warrants should be issued. I declined to conduct an ex parte meeting with the AUSA who submitted the warrants because these warrants pertain to a criminal case to which I am assigned and will be responsible for addressing any additional pretrial motions or other matters referred automatically or by order of the district judge. This order is entered to explain why I declined to authorize the search warrants requested, and to allow the government to appeal my decision to the district judge.

The caption of this order contains the case numbers issued to the search warrants issued in September 19, 2014, for these same six devices as well as the case numbers issued for these six devices when new warrants were submitted to me on February 19, 2015. The government did not reapply for search warrants for five devices recovered from Villas 8882 and 8888, which the court authorized under Case Nos. 2:14-mj-0609-PAL, 2:14-mj-0610-PAL, 2:14-mj-0615-PAL, 2:14-mj-0616-PAL and 2:14-mj-0617-PAL.

BACKGROUND

I. The September 19, 2014, Search Warrants.

On September 19, 2014, I issued eleven search warrants for eleven devices recovered from Villas 8881, 8882 and 8888. The initial eleven applications for search warrants were supported by the affidavit of Task Force Officer ("TFO") Matthew Downing. The affidavit supporting the

search warrant application for all eleven devices was identical except for identifying the Villa from which the devices were recovered. The purpose of the applications for the warrants for all eleven devices was to require Apple to assist the FBI in their search of the devices which were passcode protected. The government requested and received judicial authorization to require Apple to provide reasonable technical assistance, if the devices were in reasonable working order, to unlock the passcode protection, and to the extent possible, extract data from the devices. The government requested and received judicial authorization for Apple to copy the data from the devices onto an external hard drive or other storage medium. The initial applications provided that Apple would return the storage medium containing copied data to the FBI. Upon return, the devices would be impounded into evidence, the copied data would be searched for evidence of the enumerated crimes eventually charged in the indictment, in accordance with the provisions of a search warrant protocol described in Attachment C to the warrants and in compliance with the provisions of Rule 41 of the Federal Rules of Criminal Procedure.

The affidavit of TFO Downing supporting the warrants attached a copy of Judge Koppe's earlier warrant to support the statement of probable cause. The government also applied for and received an order sealing the affidavits and warrants based on the government's assertion "that disclosure of the information might possibly jeopardize the investigation" and that the government's "right to secrecy far outweighs the public's right to know."

Task Force Officer Downing executed certified search warrant returns for all eleven warrants on October 2, 2014, to chambers as is our local practice. The returns indicated the warrants were executed on Apple on September 22, 2014. The returns also indicated that Apple did not "honor" the search warrant issued under Case No. 2:14-mj-0617-PAL because the warrant contained an incorrect serial number for the device described. With respect to the remaining ten, the search warrant returns indicated Apple advised it would take approximately nine months to extract data from the devices.

II. The February 19, 2015, Applications for Search Warrants.

These six applications for search warrants were submitted to me rather than the magistrate judge on criminal duty. When chambers inquired why the warrants were submitted to me, staff

was advised that the warrants were "piggy back"[1] search warrant applications following up on prior search warrants I had issued. The practice in this district is for the duty magistrate judge to handle any search warrant applications which are made during that judge's duty week. However, the custom and practice in this district is to present a "piggy back" warrant to the judge who issued the original warrant on which the supplemental application depends.

III. Disclosures at February 6, 2015, Hearing.

I set a status and case management conference in the criminal case on February 6, 2015, after issuing reports and recommendations concerning motions to suppress filed by the Defendants in this case. At the hearing, the parties advised me that they had reached agreements concerning briefing deadlines for objections to the three pending reports and recommendations. I addressed counsel concerning whether additional pretrial motions would be filed and the status of discovery that may impact setting a realistic trial date. Government counsel stated that the government was in the process of conducting forensic review of computers and electronic devices and would be supplementing discovery as additional information became available. Government counsel stated that it had been informed by Apple that Apple would need approximately nine months to assist the government in its attempts to access and copy Apple devices.

Counsel for both sides had indicated that they were mutually requesting an April 13, 2015, trial date. When government counsel disclosed on the record that it needed Apple's help to access and copy certain devices, I asked government counsel whether they had requested and received judicial authorization for Apple's assistance in this regard. AUSA Silva confirmed the government had obtained judicial authorization for Apple's assistance on the record. Counsel for the Defendants responded that they were unwilling to continue the trial date for the nine month period Apple stated it needed to assist in the government's forensic examination efforts.

/ / /

/ / /

[1] A piggy back warrant is a search warrant that relies upon or follows up on a prior warrant which is typically attached to the new application.

IV. Orders Sealing September 19, 2014, Warrants.

The eleven applications and warrants remain under seal. However, the court finds that there is no longer any justification for maintaining these warrants under seal for several reasons. First, the government disclosed the existence of these warrants in open court. Second, the Defendants are aware from prior search warrant returns produced in discovery in this criminal case that all of these devices were seized pursuant to the search warrant Judge Koppe issued on July 9, 2014. Third, these devices were all listed as items subject to forfeiture in the indictment. Fourth, the affidavit and application supporting the search warrants attached Judge Koppe's earlier search warrant. This is the search warrant that resulted in the motions to suppress, four days of evidentiary hearings, and my reports of findings and recommendations. It is the same warrant I have found was fatally flawed and lacked probable cause to support the search of Villa 8882. Under these circumstances, the government's unsupported statement that disclosure of the information in the search warrants "might possibly jeopardize the investigation" and that the government's "right to secrecy far outweighs the public right to know" do not support maintaining the applications and warrants under seal. For the same reasons, the court will deny the government's request to seal the affidavit and applications for the six devices submitted to me on February 19, 2015.

DISCUSSION

The government's February 19, 2015, applications for search warrants to require Apple to provide reasonable technical assistance, if the devices are in reasonable working order, to unlock the passcode protection and to the extent possible, extract data from the devices, are denied for the reasons explained below.

First, the amended affidavits in support of the applications for search warrants do not state probable cause. The amended affidavit was submitted by Thayne A. Larson, a Special Agent of the FBI who is one of several agents participating in this investigation. Paragraph 6 of the affidavit submits that there is probable cause to believe that all six devices contain evidence, fruits, instrumentalities, or proceeds of the target offenses. The target offenses are described as violations of 18 U.S.C. § 1955 – Operating an Illegal Gambling Business; 18 U.S.C. § 1084 –

Transmission of Wagering Information; 18 U.S.C. § 3 and 18 U.S.C. § 1084 – Accessory After the Fact to the Crime of Transmission of Wagering Information; and 18 U.S.C. § 2 – Aiding and Abetting 18 U.S.C. §§ 1956 and 1957, Money Laundering; and 18 U.S.C. § 371, Conspiracy.

Paragraph 7 avers that "Wei Seng Phua, Darren Wai Kit Phua, Seng Chen Yong, Wai Kin Yong, Hui Tang, Herman Chun Sang Yeung, Yan Zhang, and Yung Keung Fan and others were involved in operating an illegal gambling business when they stayed at Villas 8881, 8882 and 8888 at Caesars Palace, 3750 S. Las Vegas Blvd., Las Vegas, Nevada, during June and July of 2014." This is a conclusion, not a statement of facts or reasonable inferences drawn from facts which establish probable cause.

Paragraph 8 relates that Special Agent Pham obtained a search warrant for Villas 8881, 8882 and 8888 at Caesars Palace from Judge Koppe on July 9, 2014, which authorized the search of evidence including computers and electronic devices. Paragraph 9 relates that the search warrant was executed by FBI and Nevada Gaming Control Agents and Task Force members on July 9, 2014. Four of the six devices for which a second warrant was requested were located in Villa 8888. Two of the six devices were located in Villa 8881.

Paragraph 10 attests that on July 29, 2014, eight Defendants were indicted for violations of 18 U.S.C. § 1084, Transmission of Wagering Information; 18 U.S.C. § 1955, Illegal Gaming; and 18 U.S.C. § 2, Aiding and Abetting.

Paragraph 11 relates that six Defendants charged in the indictment pled guilty and were sentenced on December 20, 2014. The government dismissed all charges against another Defendant, Wai Kin Yong. The Defendants identified in Paragraph 11 also agreed to forfeit money and abandon to the government all the electronic items that were seized from Villas 8881 and 8888 including the devices for which these warrants were requested. Finally, Paragraph 11 states that Defendants Wei Seng Phua and Darren Wai Kit Phua have not contested the forfeiture of the devices for which a second warrant was requested.

Paragraph 12 avers that on January 30, 2015, I "suppressed the evidence that was seized from Villa 8882" but "did not suppress the evidence seized from Villas 8881 and 8888." [2]

Paragraph 13 of the affidavit states that the six devices were forensically examined by an FBI examiner who discovered the devices were locked with a passcode. As a result, forensic exams of the devices cannot proceed without the assistance of the devices' manufacturer, Apple, Inc. Apple is able to bypass the passcode and extract data from the devices.

Based on these seven paragraphs, the government requested orders in the form of search warrants directing Apple to assist in accessing and copying data from these six devices.

Probable cause is "a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules." *Illinois v. Gates*, 462 U.S. 213, 232 (1983). The existence of probable cause is determined by an analysis of the totality of the circumstances surrounding the intrusion. *Id.* Probable cause does not deal with hard certainties, but with probabilities. *Id.*, at 241. Probable cause to search exists if there is "a fair probability that contraband or evidence of a crime will be found in a particular place." *Id.*, at 238. The Fourth Amendment requires a nexus between the item to be seized and the criminal behavior. *Warden v. Hayden*, 387 U.S. 294, 307 (1967).

Special Agent Larson's statement in Paragraph 8 of the amended affidavit that the eight named Defendants "were involved in operating an illegal gaming activity when they stayed at Villas 8881, 8882, and 8888 at Caesars Palace . . . during June and July of 2014" is a conclusion, not probable cause. Like the July 9, 2014, warrant I found fatally flawed, it lumps all of the Defendants together. It does not provide factual support for the conclusion. It does not state how the affiant reached his conclusion. It does not describe where the illegal gaming activity occurred. It does not explain what conduct each individual engaged in which amounts to a violation of the law.

[2] This is not a correct statement. I lack authority to suppress evidence in a felony case. A motion to suppress is a matter that may not be finally determined by a magistrate judge pursuant to 28 U.S.C. § 636(b)(1)(B) and LR IB 1-4(h). The motions to suppress were referred to me for a report and recommendation to the district judge. The parties have now filed objections to my reports and recommendations which the district judge has set for hearing on Monday, March 23, 2015.

Paragraph 10 attests that eight Defendants were indicted for transmission of wagering information, illegal gaming, and aiding and abetting in violation of federal law on July 29, 2014. A court deciding whether to issue a search warrant must determine whether the warrant states probable cause that a crime had been committed, and that the property to be searched will contain evidence of the criminal offenses from the information provided within the four corners of the search warrant application. The fact that the grand jury indicted the Defendants does not state probable cause for issuance of a search warrant. The grand jury found probable cause based on whatever evidence was presented to it. The court has no way of knowing what evidence was submitted to the grand jury and may not simply find that because the grand jury found probable cause to believe the Defendants committed a criminal offense and that the devices listed in the indictment should be forfeited, that probable cause exists to believe the devices contain evidence of the crimes.

Paragraph 11 indicates that one Defendant pled guilty to a felony charge of transmission of wagering information, four Defendants pled guilty to a Class A misdemeanor of accessory after the fact to transmission of wagering information, and the case against a sixth Defendant was dismissed. The affidavit does not state who admitted to doing what, whether any of the Defendants who pled guilty implicated the Phuas in illegal gaming activity, where the illegal gambling business was being conducted, how the illegal gaming activity was being conducted, or the role played by each individual charged. The affidavit contains no facts indicating the six devices recovered from Villa 8881 and 8888 were used to commit the enumerated offenses, or what facts law enforcement has to believe the devices may contain evidence of the enumerated offenses.

Second, the applications and proposed search warrants do not contain a search warrant protocol for searching for and seizing only evidence of the enumerated criminal offenses. The Warrant Clause of the Fourth Amendment categorically prohibits the issuance of any warrant except one particularly describing the place to be searched and the persons or things to be seized. *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). The purpose of the particularity requirement is to prevent general searches. *Id.* By limiting the authorization to search the specific areas and

things for which there is probable cause to search, the particularity requirement ensures that the search will be carefully tailored to its justifications, and will not become a wide-ranging, exploratory search the Fourth Amendment prohibits. The scope of a lawful search is defined by the object of the search. *Id.* The test is an objective one: would a reasonable officer have interpreted the warrant to permit the search at issue. *United States v. Gorman*, 104 F. 3d 272, 274 (9th Cir. 1996).

Search warrants must be specific. *United States v. Hill*, 459 F.3d 966, 973 (9th Cir. 2006). "Specificity has two aspects: particularity and breadth. Particularity is the requirement that the warrant must clearly state what is sought. Breadth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based." *Id.* The description of items need only be reasonably specific, rather than elaborately detailed. *Id.* In determining whether a warrant is sufficiently particular, the Ninth Circuit considers one or more of the following factors: (1) whether probable cause exists to seize all items of a particular type described in the warrant; (2) whether the warrant set out objective standards by which the executing officers can differentiate items subject to seizure from those which are not; and (3) whether the government was able to describe the items more particularly in light of the information available to it at the time the warrant was issued. *Id.*

The purpose of the Fourth Amendment's particularity requirement is to make general searches impossible and prevent "exploratory rummaging in a person's belongings." *Anderson v. Maryland*, 427 U.S. 463, 480 (1976). The need to prevent general exploratory rummaging of a person's belongings is particularly acute in document searches because, unlike requests for other tangibles, document searches tend to involve broad disclosures of the intimacy of private lives, thoughts, and transactions. *United States v. Washington*, 797 F.2d 1461, 1468 (9th Cir. 1986) (internal citations and quotations omitted). However, the Ninth Circuit has often recognized a legitimate law enforcement need to scoop up large quantities of data and sift through it carefully for concealed or disguised pieces of evidence. *See, e.g., United States v. Hill*, 459 F.3d 966 (9th Cir. 2006).

There is a well-developed body of Fourth Amendment law addressing the search and seizure of large quantities of materials to review and sort the material for items within the scope of probable cause underlying warrants. For example, in *Anderson v. Maryland*, 427 U.S. at 482 n.11, the Supreme Court recognized that "in searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized."

The Ninth Circuit has exhaustively addressed search warrants for computer and electronically stored information in a series of decisions involving grand jury investigations into illegal steroid use by Major League baseball players. Three published decisions culminated in an *en banc* decision in *United States v. Comprehensive Drug Testing, Inc.*, 621 F. 3d 1162 (9th Cir. 2010) ("*CDT III*"). There, the Ninth Circuit recognized that data individuals used to keep in the file cabinets in physical facilities are now usually stored electronically, and law enforcement faces many challenges in retrieving electronically stored information. *Id.*, at 1175. "Electronic storage facilities intermingle data, making them difficult to retrieve without a thorough understanding of the filing and classification systems used—something that can often only be determined by closely analyzing the data in a controlled environment." *Id.* Because of these challenges, the Ninth Circuit recognized that law enforcement's legitimate need to seize large quantities of data is an inherent part of the electronic search process. *Id.*, at 1177. However, the legitimate need of law enforcement for authorization to examine large quantities of electronic records "creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." *Id., at 1176.*

To address these concerns, *CDT III* updated its earlier decision in *United States v. Tamura*, 694 F.2d 591 (9th Cir. 1982) "to apply to the daunting realities of electronic searches." *Id.*, at 1177. *Tamura* preceded the dawn of the information age and involved the seizure of several boxes and dozens of file drawers of paper documents to be stored off site for documents the search warrant authorized later. *CDT III* made it clear that the procedural safeguards outlined in the *Tamura* opinion have "provided a workable framework for almost three decades" and should be applied to the realities of electronic searches. Specifically, the Court of Appeals

reiterated that wholesale seizure of voluminous documents to be sorted out for documents a search warrant authorizes the government to seize may sometimes be necessary. Although often necessary, the Ninth Circuit continues to disapprove of the wholesale seizure of documents, particularly where the government fails to return materials that were not the object of the search once they have been segregated. *Id.*

With respect to electronically stored information, *CDT III* called upon magistrate judges issuing search warrants to apply *Tamura* procedures to electronically stored information "to maintain the privacy of materials that are intermingled with seizeable materials, and to avoid turning a limited search for particular information into a general search of office file systems in computer databases." *Id.*, at 1170. Because of the unique problems inherent in the electronic search process, judicial officers should exercise greater diligence "in striking the right balance between the government's interests in law enforcement and the right of individuals to be free from unreasonable searches and seizures." *Id.*, at 1177. The Ninth Circuit concluded that "the process of segregating electronic data that is seizeable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect." *Id.*

The court will not approve a search warrant for electronically stored information that does not contain an appropriate protocol delineating what procedures will be followed to address these Fourth Amendment issues. A protocol for forensic review of a device that stores data electronically must make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

Third, according to Special Agent Larson's amended affidavit, all six devices have been forfeited and abandoned to the government. The affidavit provides no justification for issuance of a search warrant where, as here, the devices now belong to the government. Paragraph 11 of the affidavit states that the Phuas "have not contested the forfeiture" of these devices. However, this is a conclusion for which no factual support is provided. How does Special Agent Larson know this? The court has no idea. Apple's request that law enforcement obtain search warrants

before they will assist the government in accessing the devices and downloading the information is not a basis for this court to issue one. If, as the government claims, all six devices have been forfeited by those who had any interest in them, it would have been a simple matter for the government to require the prior owners of the devices to provide the government with the passcodes as a condition of their plea agreements.

Fourth, as stated earlier, the affidavit is inaccurate in stating that I suppressed any evidence in this case. I made recommendations that are now before the district judge who may adopt, modify, or overrule some or all of the recommendations. I found that the July 9, 2014, search warrant supporting the search of all three Villas was fatally flawed. I did not make a recommendation concerning suppression of evidence from Villas 8881 and 8888 because the Defendants who were occupants of those Villas had withdrawn their motions when they pled guilty.

Before the evidentiary hearing on the two motions to suppress was conducted, I held a hearing to clarify how the guilty pleas of the five Defendants and dismissal of the one Defendant's case affected the remaining issues the court must decide. The Phuas conceded that they lacked standing to assert Fourth Amendment violations personal to the occupants of Villas 8881 and 8888. However, the Phuas' motion to suppress on *Franks* grounds argued they were entitled to suppression of evidence based on a warrant which included information unlawfully obtained from all three Villas. Counsel for the Phuas filed objections to the court's Report and Recommendation (Dkt. #406) which found *Franks* violations and recommended that evidence recovered from Villa 8882 be suppressed. Darren Phua has now pled guilty and withdrawn his objections. However, Paul Phua's objections remain under submission to the district judge. The Objection (Dkt. #419) and Reply (Dkt. #441) argue that the district judge should suppress all of the fruits of Judge Koppe's July 9, 2014, search warrant under *Franks v. Delaware*, and pursuant to the court's supervisory power.

Finally, the court previously issued search warrants for these same devices. The prior search warrants relied upon the search warrant issued by Judge Koppe on July 9, 2014, which I found was fatally flawed and lacked probable cause. Presumably, the government is seeking

new search warrants because of my findings and recommendations under either the independent source or inevitable discovery exceptions to the exclusionary rule. It is well established that evidence observed during a prior illegal entry of a premises need not be suppressed where officers obtain a valid search warrant that does not rely on anything seen or discovered during the prior illegal entry. *Murray v. United States*, 487 U.S. 537, 543 (1988). This is referred to as the independent source exception. The inevitable discovery exception is an extrapolation from the independent source doctrine. *Murray* at 539. A court may admit illegally obtained evidence if the evidence would inevitably have been discovered through independent, lawful means. *Id.* For example, in *United States v. Ruckes*, 586 F.3d 713, 719 (9th Cir. 2009), the Ninth Circuit held that a loaded pistol and crack cocaine found in an illegal search of the Defendant's car was admissible because they would have been found when the car was impounded and inventoried. Neither of these two exceptions apply to these six search warrants because the affidavit does not establish probable cause to search these six devices for evidence of the enumerated crimes, let alone evidence of probable cause discovered independently of what the court has found was a fatally flawed search warrant.

For these reasons, the government's applications for a search warrants for these six devices is **DENIED**.

IT IS SO ORDERED.

Dated this 20th day of March, 2015.

PEGGY A. LEEN
UNITED STATES MAGISTRATE JUDGE